This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Canceled)

2. (Previously Presented) A method for backing-up data in a wireless network, the method comprising steps of:

selecting data within a wireless device for backup in a storage area, the storage area being accessible by the wireless device through the wireless network;

encrypting the selected data; and

sending the encrypted data to the storage area

wherein the step of sending the encrypted data to the storage area is done using a Wireless Application Protocol (WAP) technique.

3. (Previously Presented) The method according to claim 2, wherein the step of sending the encrypted data to the storage area includes a step of encapsulating the encrypted data within a SyncML document.

4. (Previously Presented) The method according to claim 2, wherein the step of sending the encrypted data to the storage area includes a step of encapsulating the encrypted data within an XML document.

5. (Previously Presented) The method according to claim 2, wherein the wireless device is one of a wireless telephone handset and a personal digital assistant.

6. (Previously Presented) The method according to claim 2, wherein the step of encrypting the selected data encrypts the selected data using a public key.

7. (Original) The method according to claim 6, wherein the public key is supplied by a Wireless Identity Module (WIM).

8. (Previously Presented) The method according to claim 2, further comprising steps of:

downloading the encrypted data from the storage area; and

decrypting the encrypted data.

9. (Original) The method according to claim 8, wherein the step of downloading the encrypted data from the storage area is done using a WAP technique.

10. (Original) The method according to claim 8, wherein the step of decrypting the encrypted data decrypts the encrypted data using a private key.

11. (Currently Amended) A method for accessing backed-up data in a wireless network from a wireless device, the method comprising steps of:

downloading the backed-up data from a storage area, the backed up data having been previously selected for backup by a user of the wireless device, the backed-up data further containing encrypted data encrypted by an encryption module upon the selection of the data, and the storage area being accessible by the wireless device through the wireless network; and

decrypting the downloaded backed-up data.

12. (Original) The method according to claim 11, wherein the step of downloading the backed-up data from the storage area is done using a Wireless Application Protocol (WAP) technique.

13. (Original) The method according to claim 11, wherein the step of decrypting the downloaded backed-up data decrypts the encrypted data using a private key.

14. (Original) The method according to claim 13, wherein the private key is supplied by a Wireless Identity Module (WIM).

15. (Original) The method according to claim 11, wherein the backed-up data is embedded in a SyncML document.

16. (Original) The method according to claim 11, wherein the backed-up data is embedded in an XML document.

17. (Original) The method according to claim 11, wherein the wireless client device is one of a wireless telephone handset and a personal digital assistant.

18. (Currently Amended) A wireless terminal device, comprising:

a memory capable of storing data;

a browser ~~that~~ capable of ~~allows~~ allowing a user of the wireless terminal device to select data for backup storage;

a backup module capable of receiving the selected data upon its selection by the browser and encrypting the selected data; and

a backup application capable of sending the encrypted selected data to a storage area that is accessible to the wireless terminal device through a wireless network.

19. (Original) The wireless terminal device according to claim 18, wherein the browser is a Wireless Application Protocol (WAP) browser.

20. (Original) The wireless terminal device according to claim 18, wherein the encrypted selected data is sent to the storage area using a Wireless Application Protocol (WAP) technique.

21. (Original) The wireless terminal device according to claim 18, wherein the encrypted selected data is encapsulated within a SyncML document.

22. (Original) The wireless terminal device according to claim 18, wherein the encrypted selected data is encapsulated within an XML document.

23. (Original) The wireless terminal device according to claim 18, wherein the wireless client device is one of a wireless telephone handset and a personal digital assistant.

24. (Previously Presented) The wireless terminal device according to claim 18, wherein the backup module encrypts the selected data using a public key.

25. (Original) The wireless terminal device according to claim 24, further comprising a Wireless Identity Module (WIM) that stores the public key.

26. (Original) The wireless terminal device according to claim 18, wherein the backup application downloads the encrypted data from the storage area,

the wireless terminal device further comprising a restore module that decrypts the encrypted data.

27. (Previously Presented) The wireless terminal device according to claim 26, wherein the encrypted data is downloaded from the storage area using a Wireless Application Protocol (WAP) technique.

28. (Original) The wireless terminal device according to claim 26, wherein the restore module decrypts the encrypted data using a private key.

29. (Original) The wireless terminal device according to claim 28, further comprising a Wireless Identity Module (WIM) that stores the private key.

30. (New) A method for backing-up and retrieving data in a wireless network, the method comprising steps of:

detecting user-selected data within a wireless device for backup in a storage area, the storage area being identifiable by a URI and being accessible by the wireless device through the wireless network;

encrypting the selected data encrypted using a public key for the user supplied by a WIM associated with the user;

embedding the encrypted data in a SyncML document;

sending the encrypted data to the storage area using a Wireless Application Protocol (WAP) technique;

accessing the encrypted data in the storage area from the wireless device using a backup application stored in the wireless device;

downloading the backed-up data from the storage area, the backed up data having been previously selected for download by the user of the wireless device;

decrypting the downloaded backed-up data using a private key supplied by the WIM associated with the user.